

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

REC'D 08 MAR 2006

WIPO

PCT


Applicant's or agent's file reference PCT1935RK025rey	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/PEA/416)	
International application No. PCT/EP 03/13109	International filing date (day/month/year) 21.11.2003	Priority date (day/month/year) 21.11.2003
International Patent Classification (IPC) or both national classification and IPC INV. H04L9/32		
Applicant PITSOS, Errikos		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 8 sheets, including this cover sheet.
 - ☐ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the opinion
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☒ Lack of unity of invention
- V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 21.06.2005	Date of completion of this report 07.03.2006
Name and mailing address of the International preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Bertolissi, E Telephone No. +49 89 2399-6959



**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. **PCT/EP 03/13109**

I. Basis of the report

1. With regard to the **elements** of the international application (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17)*):

Description, Pages

1-20 as originally filed

Claims, Numbers

1-62 as originally filed

Drawings, Sheets

1/10-10/10 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

BEST AVAILABLE COPY

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. **PCT/EP 03/13109**

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).
- (Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)*

6. Additional observations, if necessary:

IV. Lack of unity of invention

1. In response to the invitation to restrict or pay additional fees, the applicant has:

- ☐ restricted the claims.
- ☐ paid additional fees.
- ☐ paid additional fees under protest.
- ☐ neither restricted nor paid additional fees.

2. ☒ This Authority found that the requirement of unity of invention is not complied with and chose, according to Rule 68.1, not to invite the applicant to restrict or pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rules 13.1, 13.2 and 13.3 is

- ☐ complied with.
- ☐ not complied with for the following reasons:

4. Consequently, the following parts of the international application were the subject of international preliminary examination in establishing this report:

- ☐ all parts.
- ☒ the parts relating to claims Nos. 45-60.

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	45-60
	No: Claims	
Inventive step (IS)	Yes: Claims	45-60
	No: Claims	
Industrial applicability (IA)	Yes: Claims	45-60
	No: Claims	

2. Citations and explanations

see separate sheet

BEST AVAILABLE COPY

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/EP 03/13109

Cited documents

The following documents are mentioned for the first time in this written opinion; the numbering will be adhered to in the rest of the procedure:

- D1: MENEZES A J ET AL: "HASH FUNCTIONS AND DATA INTEGRITY"
- D2: US-A-4 309 569 (MERKLE RALPH C) 5 January 1982 (1982-01-05)
- D3: US-A-4 881 264 (MERKLE RALPH C) 14 November 1989 (1989-11-14)
- D4: US-A-5 903 651 (KOCHER PAUL CARL) 11 May 1999 (1999-05-11)
- D5: J. CHAPWESKE, G. MOHR: "Tree Hash Exchange format (THEX)"
- D6: R. BRANDNER, TOBIAS GONDROM, U. PORDESCH, M. TIELEMANN:
" <draft-brandner-et al-ats-00.txt> - Archive Time-Stamps Syntax (ATS)"
- D7: EP-A-0 932 109 (YEDA RES & DEV) 28 July 1999 (1999-07-28)
- D8: US-A-6 065 008 (HITCHCOCK GREGORY ET AL) 16 May 2000 (2000-05-16)
- D9: EP-A-1 164 746 (MICALI SILVIO) 19 December 2001 (2001-12-19)
- D10: PHIL ZIMMERMAN ET AL: "Introduction to Cryptography (PGP 6.5 User's Guide)"
- D11: PATRICK FEISTHAMMEL: "Explanation of the web of trust of PGP"
- D12: CARONNI G: "Walking the Web of trust"
- D13: KARL ABERER, ANWITAMAN DATTA, MANFRED HAUSWIRTH: "A decentralized public key infrastructure for customer-to-customer e-commerce"
- D14: VAL HENSON: "An Analysis of Compare-by-hash"
- D15: SRDJAN CAPKUN, LEVENTE BUTTYAN AND JEAN-PIERRE HUBAUX: "Self-Organized Public-Key Management for Mobile Ad Hoc Networks"
- D16: FARID F. ELWAILLY AND ZULFIKAR RAMZAN: "QuasiModo: More Efficient Hash Tree-Based Certificate Revocation"
- D17: PREM DEVANBU, MICHAEL GERTZ, APRIL KWONG, CHIP MARTEL, GLEN NUCKOLLS, STUART G. STUBBLEBINE: "Flexible authentication of XML documents"

BEST AVAILABLE COPY

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/EP 03/13109

IV. Lack of unity of invention

This International Examination Authority agrees with the International Search Authority and found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-31; Method and computer readable medium for managing digital data
2. Claims: 32-44, 61, 62; Method and computer readable medium for providing trust levels of signatures
3. Claims 45-60; Method for providing integrity and consistency information of digital data

The lack of unity becomes apparent **a posteriori** after taking document D1 into consideration (PCT Guidelines Chapter III-7.5) which discloses cryptographic hash functions (page 321) which are the only common feature between the first and the third group of inventions while the second group does not have any common features with the other two.

With the reference to the prior art document, the first group yields the potential special technical feature of using leaf, non-leaf and root hash values, hence solving the objective problem of verifying the content of some data, even if the total data is too big to be transferred to each client (see page 13, lines 31-35 of the description):

The second group yields the potential special technical feature of signing by a second party a first party public key which is used to certify data sent to a receiver, in the situation where the receiver trusts the second party, but it does not know the first party, hence solving the objective problem of trusting data received from an unknown party.

With the reference to the prior art document, the third group yields the potential special technical feature of transmitting a hash value from a first to a second party, hence solving the objective problem of ensuring that each user that uses some data can assure the integrity of that data without requiring the existence of a third party trusted by all the parties (see description page 18, lines 5-11).

Consequently, neither the objective problems underlying the subjects of the 3 claimed inventions, nor the solutions as defined by the special technical features described

BEST AVAILABLE COPY

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/EP 03/13109

allow for the link of a common inventive concept to be established between said inventions. In conclusion therefore the 3 groups of claims are not linked by a single general inventive concept. The application hence does not meet the requirements of unity of invention as defined in Rule 13.1 and 13.2 of the PCT.

V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

As requested by the applicant with his letter requesting an International examination with a written opinion only claims 45-60 will be considered.

Group 3 (claims 45-60)

- 1 Claim 45 is the juxtaposition of two different processes;
 - the calculation of hash value of a list and the transmission of that list to a second party;
 - comparing the received list with another locally available list by means of calculation of hash values.

1.1 The first process is well known in the art and document D10 on page 19, figure 1-7 clearly shows the process of calculating a hash starting from a document and associating the hash to the document before sending it (this step is present in figure 1-6 on page 18). The fact that the process is performed on a list cannot be considered as involving an inventive step since a list is a special type of document and use of a known technique (calculating the hash on a document) in an analogous situation (calculating the hash on a list) does not involve inventive activity (see also PCT Guidelines Chapter IV-8.7-A1.v).

1.2 The second process involves comparing lists by means of hashes. This technique is already known from document D14 (abstract). The technique is used to decide whether two blocks of data are identical to each other by comparing their hash values (see abstract, lines 3-6). Its extension to cover the case where the hash is calculated on some data contained in a list (some or all the identifications of the list) cannot be seen as involving an inventive step since this is a case of analogous use, similar to the one discussed above. The fact that the list is provided by a first party cannot be used to assess the inventiveness of the

BEST AVAILABLE COPY

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/EP 03/13109

process since the origin of the file does not play any role in the process used for comparing the contents of the two lists.

1.3 Thus, since the subject matter of claim 45 consists merely in the juxtaposition or association of known devices and processes functioning in their normal way and not producing any non-obvious synergetic working interrelationship (see also PCT Guidelines Chapter IV-8.7-B1), the subject-matter of claim 45 does not involve an inventive step and does not satisfy the criterion set forth in Article 33(3) PCT.

1.4 The applicant should notice that according to the current wording of claim 45 the hash list generated from the first party is simply provided to the second party which does not make any use of it.

2 Dependent claims 46-60 do not appear to contain any additional features or method steps which, either alone or in combination with the features or method steps of any claim to which they refer, meet the requirements of the PCT with respect to inventive step, because the subject-matter of these claims relates to minor design details and is either directly derivable from the above mentioned prior art or presents standard practice. In detail:

claim 46: see D10, figure 1-7, plaintext + signature;

claim 47, 49: if the hashes of the two document differ an action is required. The nature of the action can be implemented by the man skilled in the art as needed without requiring inventive activity;

claim 49: non inventive selection of a type of data;

claim 50: see D10, figure 1-7, where the data is hashed and signed;

claim 51: non inventive selection of a type of data;

claim 52: unclear (see later);

claim 53 : non inventive selection among a set of known possibilities;

claims 54-55: unclear (see later);

claim 56: extension of the idea of certificate servers used in PGP (see D10, page 28, lines 9-10);

claim 57-60: application of a Merkle tree see D2.

Certain defects in the international application

1. The independent claims are not properly cast in the two-part form.

BEST AVAILABLE COPY

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/EP 03/13109

2. Documents D10 and D14 have not been identified in the description (Rule 5.1(a)(ii) PCT).
3. Reference signs in parentheses are missing from the claims (Rule 6.2(b) PCT).

Certain observations on the international application

The present application does not meet the requirements of Article 6 PCT in that the matter for which protection is sought is not clearly defined. The reasons are the following:

Group 3 (claims 45-60)

- 3 In claim 45 it is unclear what is the relation between the steps which allow to associate a hash value to a list and the following steps where two lists are compared, since the first hash value is not used at all in the comparing procedure.
- 4 Claim 52 recites that a "group of clients maintains mutually consistent list by interchanging said list and any update of said list between all clients of said group", however it is not possible to understand how this is achieved, since the method in the preceding claims only allows the comparison if two lists are the same, and does not give any indication on how to synchronize the lists.
- 5 Claim 54 introduces "said set" which has no antecedent. Claim 55 also introduces the notion of sets. However in the other claims the applicant has only mentioned "lists".

BEST AVAILABLE COPY